Claims

What is claimed is:

1. A method for establishing a secret to authenticate a user comprising the steps of:

receiving a secret pattern on a graphical interface, wherein the secret pattern comprises a sequence of discrete graphical choices;

converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices;

selecting a codeword from a plurality of codewords for each value in the sequence of values to generate a sequence of codewords, the plurality of codewords being associated with an error-correcting code;

calculating a security value of a security parameter from the sequence of codewords; and

comparing the security value of the security parameter to a threshold value.

2. The method of claim 1 wherein the security parameter is entropy.

3. The method of claim 1 wherein the security parameter is minentropy.

4. The method of claim 1 further comprising the step of rejecting the secret pattern if the security value of the security parameter does not meet or exceed the threshold value.

5. The method of claim 1 further comprising, if the security value of the security parameter meets or exceeds the threshold value, the steps of:

calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets; and

hashing the sequence of codewords to produce a hash of the sequence of codewords.

6. The method of claim 5 further comprising storing the sequence of offsets for use in authenticating a user.

7. The method of claim 6 further comprising storing the hash of the sequence of codewords for use in authenticating a user.

8. The method of claim 6 further comprising transmitting the hash of the sequence of codewords to an authentication device for use in authenticating a user.

9. A method for establishing a secret to authenticate a user comprising the steps of:

receiving a secret pattern on a graphical interface, wherein the secret pattern comprises a sequence of discrete graphical choices;

converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices;

selecting a codeword from a plurality of codewords for each value in the sequence of values to generate a sequence of codewords, the plurality of codewords being associated with an error-correcting code;

calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets; and

hashing the sequence of codewords to produce a hash of the sequence of codewords.

10 The method of claim 9 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected point on the graphical interface.

11. The method of claim 10 further comprising the step of displaying an image on the graphical interface after receiving the selected point on the graphical interface, wherein each discrete graphical choice in the sequence of discrete graphical choices is associated with one of a plurality of images.

12. The method of claim 11 further comprising prompting a user by displaying one of the plurality of images on the graphical interface; and receiving a match pattern on the graphical interface for comparison with the secret pattern, wherein the match pattern comprises a sequence of match points.

13. The method of claim 12 further comprising, during or after the step of receiving the match pattern on the graphical interface, displaying the selected point associated with the image on the graphical interface.

14. The method of claim 13 further comprising, during or after the step of receiving the match pattern on the graphical interface, displaying a line from a match point to the selected point associated with the image on the graphical interface.

15. The method of claim 10 further comprising providing at least one memory cue by presenting the at least one memory cue in response to a point on the image on the graphical interface being highlighted.

16. The method of claim 15 further comprising associating a first icon from a plurality of icons with a first point on the image on the graphical interface by displaying the first icon in response to the first point being highlighted; and associating a second icon from the plurality of icons with a second point on the image on the graphical interface by displaying the second icon in response to the second point being highlighted.

17. The method of claim 10 further comprising highlighting, for each discrete graphical choice in the sequence of discrete graphical choices, a plurality of points on the graphical interface as alternative graphical choices.

18. The method of claim 9 further comprising storing the sequence of offsets for use in authenticating a user.

19. The method of claim 9 further comprising storing the hash of the sequence of codewords for use in authenticating a user.

20. A method for authenticating a user comprising the steps of:

receiving an input pattern on a graphical interface, wherein the input pattern comprises a sequence of discrete graphical choices;

converting each discrete graphical choice in the sequence of discrete graphical choices into an input value to produce a sequence of input values, wherein the sequence of input values corresponds to the sequence of discrete graphical choices;

retrieving a sequence of offsets;

summing each input value from the sequence of input values with the corresponding offset from the sequence of offsets to generate a sequence of intermediate values;

selecting a codeword from a plurality of codewords for each intermediate value in the sequence of intermediate values to generate a sequence of codewords, the plurality of codewords being associated with an error-correcting code;

hashing the sequence of codewords to produce a hash of the sequence of codewords; and

authenticating a user if the hash matches a stored hash.

21. The method of claim 20 further comprising, prior to the authenticating step, the step of retrieving a stored hash.

22. The method of claim 20 further comprising, prior to the authenticating step, the step of transmitting the hash to an authentication device.

23. The method of claim 20 wherein each input value in the sequence of input values is a binary value of fixed length.

24. The method of claim 20 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected region on the graphical interface.

25. The method of claim 20 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected point on the graphical interface.

26. The method of claim 25 further comprising displaying an image on the graphical interface after receiving the selected point on the graphical interface, wherein each discrete graphical choice in the sequence of discrete graphical choices is associated with one of a plurality of images.

27. The method of claim 25 further comprising associating an icon from a plurality of icons with a point on the graphical interface by displaying the icon when the point is highlighted.

28. The method of claim 20 wherein the graphical interface displays a fractal image.

29. The method of claim 20 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected icon from a plurality of icons on the graphical interface.

30. The method of claim 29 wherein the icon on the graphical interface represents a face.

31. The method of claim 20 further comprising the step of allowing access to a resource in response to the step of authenticating the user.

32. The method of claim 31 wherein the step of allowing access to the resource comprises allowing access to at least one of a hardware device, a computer system, a portable computer, a software application, a database, and a physical location.

33. An apparatus for establishing a secret to authenticate a user, the apparatus comprising:

a graphical interface capable of receiving graphical input, the graphical interface receiving a secret pattern as graphical input, the secret pattern comprising a sequence of discrete graphical choices;

a converter in signal communication with the graphical interface, the converter converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices;

a codeword generator in signal communication with the converter, the codeword generator producing a sequence of codewords by applying a decoding function of an error correcting code to each value in the sequence of values;

a security calculator in signal communication with the codeword generator, the security calculator calculating a security value of a security parameter from the sequence of codewords; and

a comparator in signal communication with the security calculator, the comparator comparing the security value of the security parameter to a threshold value.

34. The apparatus of claim 33 wherein the security parameter is entropy.

35. The apparatus of claim 33 wherein the security parameter is minentropy.

36. The apparatus of claim 33 further comprising:

an offset calculator in signal communication with the comparator, the offset calculator calculating, if the security value of the security parameter meets or exceeds the threshold value, an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets; and

a hasher in signal communication with the comparator, the hasher applying a hash function to the sequence of codewords to produce a hash of the sequence of codewords if the security value of the security parameter meets or exceeds the threshold value.

37. The apparatus of claim 36 further comprising a memory element in signal communication with the offset calculator, the memory element storing the sequence of offsets for use in authenticating a user.

38. The apparatus of claim 37 wherein the memory element is in signal communication with the hasher and wherein the memory element stores the hash of the sequence of codewords for use in authenticating a user.

39. An apparatus for establishing a secret to authenticate a user, the apparatus comprising:

a graphical interface capable of receiving graphical input, the graphical interface receiving a secret pattern as graphical input, the secret pattern comprising a sequence of discrete graphical choices;

a converter in signal communication with the graphical interface, the converter converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices;

a codeword generator in signal communication with the converter, the codeword generator producing a sequence of codewords by applying a decoding function of an error correcting code to each value in the sequence of values;

an offset calculator in signal communication with the codeword generator, the offset calculator calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets; and

a hasher in signal communication with the codeword generator, the hasher applying a hash function to the sequence of codewords to produce a hash of the sequence of codewords.

40. The apparatus of claim 39 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected point on the graphical interface.

41. The apparatus of claim 40 further comprising a point generator in signal communication with the graphical interface, the point generator highlighting a plurality of points on the graphical interface as alternative graphical choices for each discrete graphical choice in the sequence of discrete graphical choices.

42. The apparatus of claim 41 further comprising a memory element in signal communication with the graphical interface, the memory element containing a plurality of images and a sequence of images, wherein receiving a discrete graphical choice in the sequence of discrete graphical choices triggers the graphical interface to display the next image in the sequence of images from the plurality of images contained in the memory element.

43. The apparatus of claim 42 further comprising:

a training logic element in signal communication with the graphical interface, the training logic element prompting a user to enter a match pattern upon receiving the secret pattern by causing the graphical interface to display the first image in the sequence of images, wherein the match pattern is a sequence of match points; and

a comparator in signal communication with the graphical interface, the comparator comparing the match pattern to the secret pattern.

44. The apparatus of claim 43 wherein the training logic element, during or after receiving a match point in the sequence of match points on the graphical interface, causes the graphical interface to highlight the selected point associated with the image on the graphical interface.

45 The apparatus of claim 43 wherein the training logic element, during or after receiving a match point in the sequence of match points on the graphical interface, causes the graphical interface to display a line from the match point to the selected point associated with the image on the graphical interface.

46. The apparatus of claim 39 further comprising a memory element in signal communication with the offset calculator, the memory element storing the sequence of offsets from the offset calculator for use in authenticating a user.

47. The apparatus of claim 39 wherein the memory element is in signal communication with the hasher, the memory element storing the hash of the sequence of codewords from the hasher for use in authenticating a user.

48. An apparatus for authenticating a user, the apparatus comprising:

a graphical interface capable of receiving graphical input, the graphical interface receiving an input pattern as graphical input, the input pattern comprising a sequence of discrete graphical choices;

a converter in signal communication with the graphical interface, the converter converting each discrete graphical choice in the sequence of discrete graphical choices into an input value to produce a sequence of input values, wherein the sequence of input values corresponds to the sequence of discrete graphical choices;

a memory element in signal communication with a summer, the memory element containing a sequence of offsets;

the summer in signal communication with the converter and the memory element, the summer summing each input value from the sequence of input values with the corresponding offset from the sequence of offsets to generate a sequence of intermediate values;

a codeword generator in signal communication with the summer, the codeword generator producing a sequence of codewords by applying a decoding function of an error correcting code to each intermediate value in the sequence of intermediate values; and

a hasher in signal communication with the codeword generator, the hasher applying a hash function to the sequence of codewords to produce a hash of the sequence of codewords for use in authenticating a user.

49. The apparatus of claim 48 further comprising a comparator in signal communication with the hasher, the comparator comparing the hash of the sequence of codewords to a stored hash and producing an authentication signal if the hash of the sequence of codewords matches the stored hash.

50. The apparatus of claim 49 wherein the authentication signal enables access to a resource.

51. The apparatus of claim 50 wherein the authentication signal enables access to at least one of a hardware device, a computer system, a portable computer, a software application, a database, and a physical location.

52. The apparatus of claim 48 further comprising a communication system in signal communication with the hasher, the communication system transmitting the hash of the sequence of codewords to an authentication device and receiving an authentication signal from the authentication device if the hash of the sequence of codewords matches the stored hash.

53. The apparatus of claim 48 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected region on the graphical interface.

54. The apparatus of claim 48 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected point on the graphical interface.

55. The apparatus of claim 48 further comprising a logic element in signal communication with the graphical interface, the logic element causing the graphical interface to display a new image in response to the graphical interface receiving a discrete graphical choice from the sequence of discrete graphical choices, wherein the sequence of discrete graphical choices corresponds to a sequence of images.

56. The apparatus of claim 48 further comprising a logic element in signal communication with the graphical interface, the logic element causing the graphical interface to display at least one memory cue in response to a point on the graphical interface being highlighted.

57. The apparatus of claim 56 wherein the logic element causes a first icon from a plurality of icons to be displayed on the graphical interface in response to a first point on the image on the graphical interface being highlighted; and wherein the logic element causes a second icon from the plurality of icons to be displayed on the graphical interface in response to a second point on the image on the graphical interface being highlighted.

58. The apparatus of claim 48 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected icon from a plurality of icons displayed on the graphical interface.

59. A method for generating a cryptographic secret from a visual password, the method comprising the steps of:

receiving a secret pattern on a graphical interface, wherein the secret pattern comprises a sequence of discrete graphical choices;

converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices;

selecting a codeword from a plurality of codewords for each value in the sequence of values to generate a sequence of codewords, the plurality of codewords being associated with an error-correcting code; and

manipulating the sequence of codewords to produce a cryptographic secret.

60. The method of claim 59 further comprising calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets for use in re-generating the secret.

61. The method of claim 59 wherein the selecting step comprises applying a decoding function of an error-correcting code to each value in the sequence of values to generate a sequence of codewords.

62. The method of claim 59 wherein the manipulation step comprises applying a hash function to the sequence of codewords.

63. The method of claim 59 further comprising using the cryptographic secret as an encryption key.

64. The method of claim 59 further comprising using the cryptographic secret in a digital signature algorithm or an identification algorithm.